CLAIMS

1. A method of joining a first device to a radio communications network controlled by a second device without contemporaneous user input of a secret at the second device, comprising:
storing in the second device a secret generated at the second device;
making the stored secret available at the first device; and
creating in the first device and in the second device, using the secret, a secret key for use in securing communication between the first and second devices.

2. A method as claimed in claim 1, wherein the secret is previously generated at the second device by user input to the second device.

3. A method as claimed in claim 1 or 2, wherein the stored secret is associated with an operational mode of the device.

4. A method as claimed in claim 1 or 2, wherein the stored secret is associated with a service provided by the device.

5. A method as claimed in any preceding claim, further comprising, at the second device, receiving a signal from the first device and in response to the received signal, automatically creating without user intervention the secret key.

6. A method as claimed in any preceding claim, where making the stored secret available at the first device is without communication in the network.

7. A method as claimed in any preceding claim, wherein making the stored secret available at the first device involves user input of the secret to the first device.

8. A method as claimed in any preceding claim further comprising storing in the second device an identifier of the first device and an identifier of the second device.

9. A method as claimed in any preceding claim, wherein the step of creating the secret key uses a random number communicated between the first and second devices.

10. A method as claimed in any preceding claim, wherein the step of creating the secret key uses an identifier of one of the first and second devices, communicated between the first and second devices, in the creation of the secret key.

11. A method as claimed in any preceding claim, further comprising:
re-using the stored secret to join a third device to the radio communications network without contemporaneous user input of a secret at the second device, comprising:
making the stored secret available at the third device; and
creating in the third device and in the second device, using the secret, a secret key for securing communication between the third and second devices.

12. A method of joining a plurality of first devices to a radio communications network controlled by a second device, comprising:
storing in the second device a generated secret at the second device;
making the stored secret available to each of the first devices; and
creating in the first devices and in the second device, using the secret, at least one secret key for use in securing communication between the first devices and the second device.

13. A method as claimed in claim 12, wherein the step of creating at least one secret key comprises:
creating a plurality of secret keys distributed across the first devices by creating a different secret key at each of the plurality of first devices; and
creating an identical plurality of secret keys at the second device.

14. A device for controlling a radio communications network comprising the device and one or more additional devices, the device comprising:
a user interface for generating a secret by user input;
a memory for storing a generated secret for use in securing communications in the network;
a radio transceiver for communicating in the network; and
a processor for accessing the secret stored in the memory and for creating, using the accessed secret, a secret key for securing communication.

15. A device as claimed in claim 14, wherein the stored secret is generated by user input using the user interface.

16. A device as claimed in claim 14 or 15, wherein stored secret is associated with an operational mode of the device.

17. A device as claimed in claim 14, or 15, wherein stored secret is associated with a service provided by the device

18. A device as claimed in any one of claims claim 14 to 17, wherein the radio transceiver is operable to receive a signal from any one of the additional devices and the processor is operable to access the secret in the memory in response to the received signal and create the secret key.

19. A device as claimed in claim 18, wherein the processor is operable to automatically create the secret key in response to the received signal.

20. A device as claimed in claim 18 or 19, wherein the stored secret is independent of the origin of the received signal.

21. A device as claimed in any one of claims 14 to 20, wherein the secret key is dependent upon the origin of the received signal.

22. A device as claimed in any one of claims 14 to 21, wherein the received signal is a request and the secret key is dependent upon the content of the received request.

23. A device as claimed in claim 22, wherein the request includes a random value used with at least the stored secret to create the secret key

24. A device as claimed in any one of claims 14 to 23, wherein the processor is operable in a first mode to obtain a secret by accessing the secret stored in the memory, is operable in a second mode to obtain a secret by enabling user input of data, and is operable in the first mode and in the second mode to create, using the obtained secret, the secret key for securing communication.

25. A device as claimed in claim 24, wherein the first mode is an interactive gaming mode and second mode is an idle mode

26. A device as claimed in any one of claims 14 to 25, wherein the memory stores a device identifier for use with at least the stored secret to create the secret key.

27. A device as claimed in any one of claims 14 to 26, further comprising a user input device for programming the value of the stored secret.

28. A device as claimed in any one of claims 14 to 28, wherein the secret key is for use in securing all communications in the network.

29. A device as claimed in any one of claims 14 to 28, wherein the memory is for storing a secret for use in securing communications in the network between the device and a first additional device and between the device and a second additional device, the processor is for accessing the secret in the memory and for creating, using the secret, a first secret key in common with the first additional device for securing communication between the device and the first additional device and a second secret key in common with the second

additional device for securing communication between the device and the second additional device.

30. A device as claimed in any one of claims 14 to 29, further comprising a user interface for entering data, wherein when the device participates in a different network controlled by a different device the user interface is usable to enter a secret stored at the different device and the processor is operable to create, using the entered secret, a secret key for securing communication.

31. A radio communications network having a common secret for re-use in securing communications in the network, the network comprising :
a controlling device, for creating the network, comprising:
a user interface for user input of a common secret;
a memory for storing a common secret;
a first radio transceiver for communicating in the network; and
a first processor for accessing the common secret stored in the memory and for creating, using the accessed common secret, a secret key for securing communication, and
a participating device, for participating in the network, comprising:
input means for inputting the stored common secret to the participating device;
a second radio transceiver for communicating in the network; and
a second processor for creating, using the input common secret, the secret key for securing communication.

32. A radio communications network as claimed in claim 31, wherein the participating device transmits a signal to the controlling device and the controlling device responds by automatically creating the secret key, without user intervention.

33. A radio communications network having a common secret for re-use in securing communications in the network, the network comprising
a controlling device, for creating the network, comprising:
a user interface for user input of a common secret;

a memory for storing a common secret;

a first radio transceiver for communicating in the network; and

a first processor for accessing the stored common secret in the memory and for creating, using the stored common secret, secret keys for securing communication between the controlling device and each of a plurality of participating devices, and

a plurality of participating devices, for participating in the network, each comprising:

input means for inputting a common secret to the participating device;

a second radio transceiver for communicating in the network; and

a second processor for creating, using the input common secret, a secret key for securing communication dependent upon the participating device and identical to one of the secret keys created in the controlling device.